

Response to First Office Action
Docket No. 002.0200.US.UTL

REMARKS

Claims 1-30 are pending. Claims 1, 11, 22, and 26 have been amended.
Claims 1-30 remain in the application. No new matter has been entered.

Claims 1-2, 4-6, 8-12, 14-18, and 20-21 stand rejected under 35 U.S.C.
5 §102(e) as being anticipated by U.S. Patent No. 6,256,668, issued to Slivka et al.
("Slivka"). Applicant traverses the rejection.

A claim is anticipated under 35 U.S.C. §102(e) only if each and every
element as set forth in the claim is found, either expressly or inherently described,
in a single prior art reference. MPEP § 2131. The Slivka reference fails to
10 describe, either expressly or inherently, each and every claim element of, and
therefore does not anticipate, Claims 1-2, 4-6, 8-12, 14-18, and 20-21.

Slivka describes a method for identifying and obtaining computer software
that operates when a user, who has purchased or downloaded free computer
software, calls an update service or network service provider on a periodic basis
15 (Abstract; Col. 2, lines 32-37; Col. 6, lines 11-28; FIGURE 4). A user contacts a
remote update service or network service ("update service"), also referred to as a
network browser service (Col. 11, lines 61-64). One or more databases connected
to update service computers are used to store database entries consisting of
computer software available on the update service computers (Col. 5, lines 34-
20 37). Upon connection, the update service conducts an automatic inventory of the
computer software on the user computer and the data collected from the inventory
is used to make a comparison to database entries from the databases containing
information about computer software then available (Col. 2, lines 37-44; Col. 6,
lines 29-39; FIGURE 4). After the comparison is complete, the update service
25 sends a summary to the user computer to alert the user to the availability of the
new or enhanced computer software and makes the computer software stored at a
remote update service computer available to the user (Col. 2, lines 49-52; Col. 6,
lines 39-54; Col. 11, lines 64-67; FIGURE 4).

In contrast, amended Claim 1 recites a self-extracting configuration file
30 containing an executable configuration file that is self-extractable on a target

Response to First Office Action
Docket No. 002.0200.US.UTL

client into a security application that is remotely administered *by an administrator system*. Claim 1 further recites an executable control embedded within an active administration Web page, the executable control being triggered upon each request for the active Web page *by the administrator system* and causing *dynamic* Web content to be generated therefrom. Claim 1 further recites a Web server exporting a Web portal comprising the active administration Web page to a browser application *on the administrator system* independent of a specific operating environment (emphasis added). Such limitations are neither taught nor suggested by Slivka.

10 In particular, Claim 1 recites triggering an executable control in an active administration Web page by an administrator system, rather than checking for and alerting a user of new and additional software upon receiving an update request from a user computer that also receives the update or modification, as described by Slivka. By allowing an administrator system to trigger the active

15 administration Web page, a third party computer system, that is, the administrator system, is able to cause the copying of a self-extracting configuration file to a target client that is self-extractable into a security application that is remotely administered by the administrator system. In contrast, Slivka discloses self-administration by a user computer. Additionally, Claim 1 recites exporting a Web

20 portal to a browser application on the administrator system independent of a specific operating environment, rather than sending a summary to the user computer containing information about computer software available on the update service computer, as described by Slivka. The exported Web portal allows the administrator system to cause the Web server to copy the self-extracting

25 configuration file to the target client as a “push” installation, unlike Slivka, which discloses “pull” installations. Finally, Claim 1 recites dynamically generating Web content upon the triggering of the executable control, rather than only maintaining a database of software available as of the time of the user update request, as disclosed by Slivka. Support for the amendments can be found in the

30 specification on page 5, line 4 through page 6, line 2; page 6, lines 11-24.

In contrast, amended Claim 11 recites storing a self-extracting

Response to First Office Action
Docket No. 002.0200.US.UTL

configuration file containing an executable configuration file that is self-extractable on a target client into a security application that is remotely administered by an *administrator system*. Claim 11 further recites providing an executable control embedded within an active administration Web page, the
5 executable control being triggered upon each request for the active Web page by the *administrator system* and causing *dynamic* Web content to be generated therefrom. Claim 11 further recites exporting a Web portal comprising the active administration Web page to a browser application *on the administrator system* independent of a specific operating environment (emphasis added). Such
10 limitations are neither taught nor suggested by Slivka.

In particular, Claim 11 recites triggering an executable control in an active administration Web page by an administrator system, rather than checking for and alerting a user of new and additional software upon receiving an update request from a user computer that also receives the update or modification, as described
15 by Slivka. By allowing an administrator system to trigger the active administration Web page, a third party computer system, that is, the administrator system, is able to cause the copying of a self-extracting configuration file to a target client that is self-extractable into a security application that is remotely administered by the administrator system. In contrast, Slivka discloses self-
20 administration by a user computer. Additionally, Claim 11 recites exporting a Web portal to a browser application on the administrator system independent of a specific operating environment, rather than sending a summary to the user computer containing information about computer software available on the update service computer, as described by Slivka. The exported Web portal allows the
25 administrator system to cause the Web server to copy the self-extracting configuration file to the target client as a "push" installation, unlike Slivka, which discloses "pull" installations. Finally, Claim 11 recites dynamically generating Web content upon the triggering of the executable control, rather than only maintaining a database of software available as of the time of the user update
30 request, as disclosed by Slivka. Support for the amendments can be found in the specification on page 5, line 4 through page 6, line 2; page 6, lines 11-24.

Response to First Office Action
Docket No. 002.0200.US.UTL

Claims 2, 4-6, and 8-10 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 12, 14-18, and 20-21 are dependent on Claim 11 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Withdrawal of the rejection under 35 U.S.C. §102(e) is respectfully requested.

Claims 3, 7, 13, 19, and 22-30 stand rejected under 35 U.S.C. §103(a) as being obvious over Slivka, in view of U.S. Patent No. 6,742,026, issued to Kraenzel et al. ("Kraenzel"). Applicant traverses the rejection.

To establish a *prima facie* case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there must be a reasonable expectation of success; and (3) the combined references must teach or suggest all the claim limitations. MPEP §2143. A *prima facie* case of obviousness has not been shown.

In particular, a *prima facie* case of obviousness has not been shown with respect to Claims 22 and 26. Amended Claim 22 recites an executable control embedded into an active administration Web page, the executable control being triggered upon each request for the active Web page by a requesting administrator and causing dynamic Web content to be generated therefrom. Claim 22 further recites a Web server serving the active administration Web page to a browser application to the requesting administrator (emphasis added). Such limitations are neither taught nor suggested by Slivka.

In particular, Claim 22 recites triggering an executable control in an active administration Web page by an administrator system, rather than checking for and alerting a user of new and additional software upon receiving an update request from a user computer that also receives the update or modification, as described by Slivka. By allowing an administrator system to trigger the active administration Web page, a third party computer system, that is, the administrator system, is able to cause the copying of a self-extracting configuration file to a target client that is self-extractable into a security application that is remotely

Response to First Office Action
Docket No. 002.0200.US.UTL

administered by the administrator system. In contrast, Slivka discloses self-administration by a user computer. Additionally, Claim 22 recites serving the active administration Web page to a browser application on the administrator system, rather than sending a summary to the user computer containing
5 information about computer software available on the update service computer, as described by Slivka. The exported Web portal allows the administrator system to cause the Web server to copy the self-extracting configuration file to the target client as a "push" installation, unlike Slivka, which discloses "pull" installations. Finally, Claim 22 recites dynamically generating Web content upon the triggering
10 of the executable control, rather than only maintaining a database of software available as of the time of the user update request, as disclosed by Slivka. Support for the amendments can be found in the specification on page 5, line 4 through page 6, line 2; page 6, lines 11-24.

Similarly, amended Claim 26 recites an executable control embedded into
15 an active administration Web page, the executable control being triggered upon each request for the active Web page *by a requesting administrator* and causing *dynamic* Web content to be generated therefrom. Claim 26 further recites a Web server serving the active administration Web page to a browser application *to the requesting administrator* (emphasis added). Such limitations are neither taught
20 nor suggested by Slivka.

In particular, Claim 26 recites triggering an executable control in an active administration Web page by an administrator system, rather than checking for and alerting a user of new and additional software upon receiving an update request from a user computer that also receives the update or modification, as described
25 by Slivka. By allowing an administrator system to trigger the active administration Web page, a third party computer system, that is, the administrator system, is able to cause the copying of a self-extracting configuration file to a target client that is self-extractable into a security application that is remotely administered by the administrator system. In contrast, Slivka discloses self-
30 administration by a user computer. Additionally, Claim 26 recites serving the active administration Web page to a browser application on the administrator

Response to First Office Action
Docket No. 002.0200.US.UTL

5 system, rather than sending a summary to the user computer containing information about computer software available on the update service computer, as described by Slivka. The exported Web portal allows the administrator system to cause the Web server to copy the self-extracting configuration file to the target client as a "push" installation, unlike Slivka, which discloses "pull" installations. Finally, Claim 26 recites dynamically generating Web content upon the triggering of the executable control, rather than only maintaining a database of software available as of the time of the user update request, as disclosed by Slivka. Support for the amendments can be found in the specification on page 5, line 4
10 through page 6, line 2; page 6, lines 11-24.

Claims 23-25 are dependent on Claim 22 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 27-30 are dependent on Claim 26 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein.

15 In addition, Claims 3 and 7 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 13 and 19 are dependent on Claim 11 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of
20 the rejection of Claims 3, 7, 13, 19, and 22-30 for obviousness under 35 U.S.C. 103(a) is requested

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

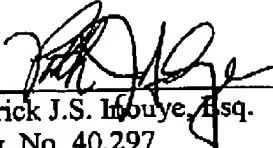
25 Claims 1-30 are believed to be in condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Response to First Office Action
Docket No. 002.0200.US.UTL

Respectfully submitted,

Dated: December 8, 2004

By:


Patrick J.S. Inouye, Esq.
Reg. No. 40,297

5
10 Law Offices of Patrick J.S. Inouye
810 Third Avenue, Suite 258
Seattle, WA 98104

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

OA Response

OA Response

- 14 -